2024 March, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at info@blackcell.io.

List of Contents

ICS podcasts

People listen more and more podcasts nowadays. Whether it's for our personal interests or for our professional development, the world of podcasts is a great possibility to be well informed. In this section, we bring together the ICS security podcasts from the previous month.

Dale Peterson

- S4x24 Preview

Link: https://dale-peterson.com/podcast-2/

Industrial Cybersecurity Pulse

- Ep. 41: Itzik Kotler on the ABC's of Cybersecurity
- Ep. 42: Lesley Carhart on the Impact of AI on Cybersecurity
- Ep. 43: Xavier Mesrobian on connecting OT and IT

Link: https://www.industrialcybersecuritypulse.com/ics-podcast/

Industrial Defender

Many podcasts available from 2023 on the following link in these themes:

- The Importance of OT Security,
- Bridging IT and OT,
- Best Practice & Compliance Frameworks,
- Vulnerabilities and Risk.

Link: The PrOtect OT Cybersecurity Podcast: 2023 Wrapped | Industrial Defender OT/ICS Cybersecurity Blog

ICS Cyber Talks Podcast

- Nachshon Pincu hosts Itay Yanovski and Nimrod Luria Co-Founders and CEOs at IO01. Both are well known in the Israeli cyber industry as successful Entrepreneurs with their cybersecurity startups for the last two decades, in a conversation about OT cybersecurity defense and the importance of hands-on training for ICS/OT cyber specialists.

- Nachshon Pincu hosts Chen Girat, the CISO of the Israel Electric Company (IEC), who started his career in cyber at the State Authority for Information Security, the base from which the Israel National Cyber Directorate grew, and managed the operations division INCD in a conversation about protecting the most significant critical infrastructure in Israel in general and during the war in particular.
- Nachshon Pincu hosts Roni Roytman, an expert in cyber crisis management and serial entrepreneur, co-founder, and CEO of companies dealing in cyber security and crisis management. In a conversation about the cybernetic war that has been at peak intensity since October 7th. Attacks on all sectors, including operational systems.

Link: https://icscybertalks.podbean.com/

BEERISAC: OT/ICS Security Podcast Playlist

- Top Gun Meets the Cloud: Ken's Guide to Keeping Your Airplanes (and Data) Safe
- The future of OT Security is so exciting' with Danielle Jablanski OT Cybersecurity Strategist
- CISA's Critical Infrastructure Protection Mission with Jen Easterly
- Feeding the Digital Age: Part 2 - Embracing Solutions
- Securing Critical Infrastructure: Challenges and Strategies with Sean Tufts
- We get what we ask for
- Keeping the Lights On: Carlos's Roadmap to Becoming an Energy Cybersecurity Pro
- OT Security's Digital Makeover
- Operational Technology disruptions: An eye on the water sector
- OT Security Made Simple | Wer ist für Security by Design zuständig? (nicht wer du denkst)
- Roni Roytman Co-founder & CEO @INTENSITY about Cyberwar since October 7th: OT cyber attacks are here
- Cybersecurity in the AVEVA Enterprise SCADA Product - Going Deep [The Industrial Security Podcast]
- Mike Rogers on Understanding a CISO's Personal Exposure in Cyber Incidents
- Where to start!?
- Defending Our Crown Jewels: Rail Cybersecurity in the Age of Industry 4.0
- OT Security Made Simple | What is Zero Trust really (and does it work in OT)?

- Mastering Data Complexity: Insights from Chase Richardson and Martin Riley on OT Integration
- Volt Typhoon and the Year in Review
- Defensible Architecture: Crafting Your Security Blueprint with Harry Thomas, Founder & CS/OT Cybersecurity Expert
- Palo Alto Networks Talks IT/OT Convergence
- Cybercrime Wire For Feb. 27, 2024. Cyberattack Hits German Steel Conglomerate. WCYB Digital Radio

Link: https://www.iheart.com/podcast/256-beerisac-ot-ics-security-p-43087446/

ICS good practices, recommendations

A Comprehensive Guide to SCADA Cybersecurity

Claroty published an article outlining challenges and cybersecurity best practices in SCADA security.

According to the publisher the challenges to SCADA Cybersecurity are the followings:

1. Legacy Systems
2. IT/OT Convergence
3. Traditional IT Tools
4. Remote Access
5. Regulatory Requirements

SCADA Cybersecurity Best Practices:

1. Gain visibility into your ICS environment

Implementing a robust SCADA cybersecurity strategy begins with gaining visibility across your entire environment, which includes creating a comprehensive inventory of assets and systems. However, achieving full-spectrum visibility poses significant challenges due to the diverse mix of devices, ineffective traditional IT tools, and the unique complexities of each critical infrastructure environment, emphasizing the importance of partnering with a cyber-physical systems (CPS) security provider offering flexible discovery methods tailored to your specific needs.

2. Integrate your existing IT tools and workflow with your ICS

After achieving enterprise-wide visibility, organizations must integrate their existing IT tools and workflows with OT. Many CPS environments have legacy devices using proprietary protocols, such as SCADA, incompatible with traditional IT security solutions. Traditional vulnerability scanners pose risks, and patching is often restricted, necessitating specialized security controls and collaboration between IT and OT security teams to protect against cyber-attacks. Partnering with a CPS security solution that integrates seamlessly with existing tech stacks enables organizations to extend their tools and workflow from IT to OT effortlessly.

3. Extend your IT security controls and governance to your ICS environment

Most ICS environments lack essential cybersecurity controls and governance, as legacy industrial devices like SCADA were initially designed for functionality rather than security, resulting in a lack of awareness about the unique challenges of interconnected ICS environments. Without dedicated security teams or specialized

solutions, organizations face inconsistent governance and control. Partnering with a CPS security vendor can provide visibility into all ICS, integrate existing IT tools with OT, and unify security governance to achieve cyber and operational resilience.

SCADA systems play a vital role in industrial efficiency and decision-making but are increasingly vulnerable to cyber-attacks. To mitigate risks, organizations must align cybersecurity practices with evolving threats, implement best practices, and partner with trusted security vendors to safeguard critical infrastructure.

Source, and more information available on the following link:

https://claroty.com/blog/a-comprehensive-guide-to-scada-cybersecurity

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in April 2024:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

- Operational Security (OPSEC) for Control Systems (100W)
- Differences in Deployments of ICS (210W-1)
- Influence of Common IT Components on ICS (210W-2)
- Common ICS Components (210W-3)
- Cybersecurity within IT & ICS Domains (210W-4)
- Cybersecurity Risk (210W-5)
- Current Trends (Threat) (210W-6)
- Current Trends (Vulnerabilities) (210W-7)
- Determining the Impacts of a Cybersecurity Incident (210W-8)
- Attack Methodologies in IT & ICS (210W-9)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10)
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11)
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115)
- ICS410: ICS/SCADA Security Essentials
- ICS515: ICS Active Defense and Incident Response

https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/#training-and-pricing

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)
- An Introduction to the DNP3 SCADA Communications Protocol
- Learn SCADA from Scratch - Design, Program and Interface

https://www.udemy.com/ics-scada-cyber-security/

- SCADA security training

https://www.tonex.com/training-courses/scada-security-training/

- Fundamentals of Industrial Control System Cyber Security
- Ethical Hacking for Industrial Control Systems

https://scadahacker.com/training.html

- INFOSEC-Flex SCADA/ICS Security Training Boot Camp

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

- Industrial Control System (ICS) & SCADA Cyber Security Training

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

- Bsigroup: Certified Lead SCADA Security Professional training course

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

- The Industrial Cyber Security Certification Course

https://prettygoodcourses.com/courses/industrial-cybersecurity-professional/

- Secure IACS by ISA-IEC 62443 Standard

https://www.udemy.com/course/isa-iec-62443-standard-for-secure-iacs/

- Dragos Academy ICS/OT Cybersecurity Training

https://www.dragos.com/dragos-academy/#on-demand-courses

- ISA/IEC 62443 Training for Product and System Manufacturers

https://www.ul.com/services/isaiec-62443-training-product-and-system-manufacturers?utm_mktocampaign=cybersecurity_industry40&utm_mktoadid=635856951086&campaignid=18879148221&adgroupid=143878946819&matchtype=b&device=c&creative=635856951086&keyword=industrial%20cyber%20security%20training&gclid=EAIaIQobChMI2sLO8fyv_AIVWvZ3Ch0b-QJvEAMYAyAAEgJNkvD_BwE

- ICS/SCADA/OT Protocol Traffic Analysis: IEC 60870-5-104

https://www.udemy.com/course/ics-scada-ot-protocol-traffic-analysis-iec-60870-5-104/

- NIST(800-82) Industrial Control system(ICS) Security

https://www.udemy.com/course/nist800-82-industrial-control-systemics-security/

- ICS/OT Cybersecurity All in One as per NIST Standards

https://www.udemy.com/course/ics-cybersecurity/

NEW! in this feed:

- Lead SCADA Security Manager

https://pecb.com/en/education-and-certification-for-individuals/scada/lead-scada-security-manager

ICS conferences

In April 2024, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

Cyber Security for Critical Assets APAC Summit

The Cyber Security for Critical Assets APAC Summit is returning to Singapore for its 5th annual edition on 3-4th April 2024. This time, the event will run in conjunction with the newly launched APAC Cyber Summit. While the former brings together critical infrastructure industries with a strong focus on OT/ICS security, the latter is the prime cross-industry conference dedicated to IT and enterprise security. This is an exclusive, English-language joint-event, with the number one aim of bringing together 150+ like-minded, senior cyber security leaders and decision-makers from industries such as Oil & Gas, Mining, Utilities, Manufacturing and Transportation, as well as Finance, Healthcare, Retail and more to connect, learn, be inspired and collaborate on building cyber resilience.

Singapore, Singapore; 3rd – 4th April 2024

More details can be found on the following website:

https://apac.cs4ca.com/

18. International Conference on Cyber Security of Industrial Control Systems

The International Research Conference is a federated organization dedicated to bringing together a significant number of diverse scholarly events for presentation within the conference program. Events will run over a span of time during the conference depending on the number and length of the presentations. With its high quality, it provides an exceptional value for students, academics and industry researchers. International Conference on Cyber Security of Industrial Control Systems aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyber Security of Industrial Control Systems. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Cyber Security of Industrial Control Systems.

Venice, Italy; 4th – 5th April 2024

More details can be found on the following website: https://waset.org/cyber-security-of-industrial-control-systems-conference-in-april-2024-in-venice?utm_source=conferenceindex&utm_medium=referral&utm_campaign=listing

15th SCADA World Summit

Following the success of the SCADA Summit World Series, the world's leading 15th SCADA World Summit 2024 will take place in person this coming 16-19 April 2024. This is the premier networking and learning platform for decision makers & specialists from the Energy & Utilities, Water & Wastewater, Industrial Manufacturing & Transportation Sectors as well as government agencies globally to discuss and share insightful experiences and knowledge on SCADA system design, engineering, planning, implementation, maintenance, digitalization, network analysis and also security management!

Singapore, Singapore; 16th – 19th April 2024

More details can be found on the following website:

https://www.equip-global.com/scada-world-summit-2024

ICS incidents

Cyberattack on Change Healthcare - Service Disruption and Recovery Efforts

Change Healthcare, a crucial component of the UnitedHealth Group, finds itself grappling with a significant cyberattack initiated by a suspected nation-state associated cyber threat actor. The incident, which commenced on the 21st of February, has led to widespread disruptions in essential services, prompting urgent efforts to restore normal operations.

Initial investigations revealed unauthorized access by malicious actors to certain information technology systems within Change Healthcare. Prompt action was taken to isolate affected systems and contain the threat. UnitedHealth Group, in collaboration with security experts and law enforcement agencies, is actively investigating the incident to ascertain the extent of the breach and mitigate potential risks.

The disruption has resulted in the unavailability of several critical services, affecting healthcare providers, pharmacies, and consumers nationwide. While specific details regarding the duration and extent of the disruption remain unclear, Change Healthcare is working tirelessly to expedite the restoration process without compromising security measures.

In response to the incident, precautionary measures have been advised for healthcare organizations, urging temporary disconnection from Optum services if potential risks are suspected. The American Hospital Association has issued cybersecurity advisories, recommending proactive measures to mitigate potential threats.

Despite the challenges posed by the cyberattack, Change Healthcare remains committed to ensuring uninterrupted access to essential healthcare resources. Dedicated teams are actively engaged in coordination with stakeholders, including customers, clients, and government agencies, to address concerns and provide necessary support.

As the situation evolves, regular updates will be provided to stakeholders to ensure transparency and effective communication. In the interim, affected parties are encouraged to explore alternative workflows and contingency plans to minimize disruptions and uphold the integrity of healthcare services.

Change Healthcare acknowledges the inconvenience caused by the cyberattack and appreciates the patience and cooperation of stakeholders during this challenging

period. Rest assured, every effort is being made to resolve the issue promptly and effectively, safeguarding the integrity of healthcare operations.

For further updates and assistance, stakeholders are encouraged to refer to the dedicated incident page or reach out to the support team.

The sources are available on the following links:

https://www.pymnts.com/news/security-and-risk/2024/change-healthcare-expects-cyberattack-disruption-through-friday/

https://www.hfma.org/technology/cybersecurity/cyberattack-on-change-healthcare-brings-turmoil-to-healthcare-operations-nationwide/

https://www.medicaleconomics.com/view/change-healthcare-s-computer-systems-down-for-sixth-day

Book recommendation

Industrial Cybersecurity: Case Studies and Best Practices

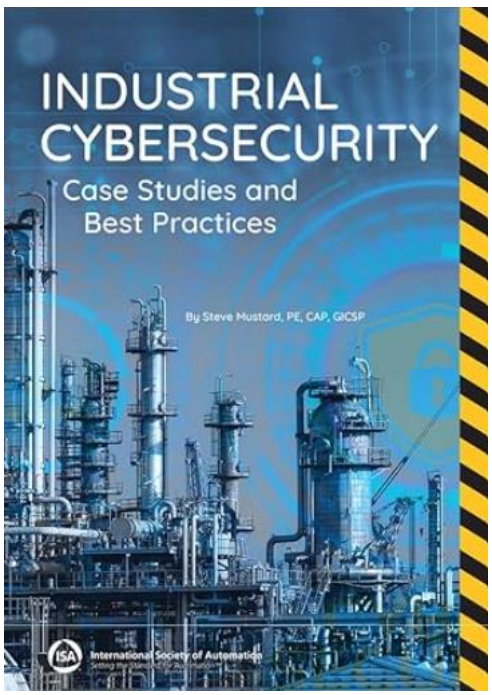
This book provides a practical overview of industrial control systems cybersecurity from governance through design and implementation to operational support. It is for anyone involved in industrial control systems cybersecurity, including asset owners, vendors, system integrators, and consultants, regardless of their level of technical expertise. The term "industrial control systems" is very broad and in this context, includes any system that is used to monitor or control physical equipment such as building control systems (e.g., heating, ventilation, and air conditioning systems), water treatment plant supervisory control and data acquisition (SCADA) systems, oil and gas distributed control systems (DCSs), and safety instrumented systems (SISs). The author explains each phase of the process of designing, implementing, and maintaining a successful cybersecurity system, as well as the underlying issues that must be addressed. He emphasizes that the key to success is support and participation from everyone—just like successful safety programs.

Author/Editor: Steve Mustard (Author)

Year of issue: 2022

The book is available at the following link:

https://www.amazon.com/Industrial-Cybersecurity-Case-Studies-Practices/dp/1643311549



ICS security news selection

The Week in Ransomware - March 1st 2024 - Healthcare under siege

Ransomware attacks on healthcare over the last few months have been relentless, with numerous ransomware operations targeting hospitals and medical services, causing disruption to patient care and access to prescription drugs in the USA.

The most impactful attack of 2024 so far is the attack on UnitedHealth Group's subsidiary Change Healthcare, which has had significant consequences for the US healthcare system. This attack was later linked to the BlackCat ransomware operation, with UnitedHealth also confirming the group was behind the attack.

Change Healthcare is an electronic payment exchange service used by doctors, pharmacists, and hospitals to submit billing claims in the US healthcare system. …

Source and more information:

https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-march-1st-2024-healthcare-under-siege/

Remote Stuxnet-Style Attack Possible with Web-Based PLC Malware: Researchers

A team of researchers has developed malware designed to target modern programmable logic controllers (PLCs) in an effort to demonstrate that remote Stuxnet-style attacks can be launched against such industrial control systems (ICSs).

The researchers are from the Georgia Institute of Technology and they have published a paper detailing this ICS security project.

In the case of traditional PLCs, an attacker can target the control logic layer or the firmware layer. Firmware attacks can provide a high level of device control and are difficult to detect, but the malware can be challenging to deploy. Control logic malware is easier to deploy, but also easier to detect. Both of these scenarios require the attacker to have privileged access to the targeted organization’s industrial network. …

Source and more information:

https://www.securityweek.com/remote-stuxnet-style-attack-possible-with-web-based-plc-malware-researchers/

UK Government Releases Cloud SCADA Security Guidance

UK's NCSC releases security guidance for OT organizations considering migrating their SCADA solutions to the cloud.

The UK's National Cyber Security Centre (NCSC) released security guidance on Monday to help organizations that use operational technology (OT) determine whether they should migrate their supervisory control and data acquisition (SCADA) systems to the cloud.

SCADA systems have traditionally been isolated from the internet and even the local enterprise network for security reasons, but the cloud can offer numerous benefits and many organizations are taking the cloud into consideration.

The guidance published by the NCSC aims to help OT organizations identify the benefits and challenges of cloud-hosted SCADA, and enable them to make a risk-based decision before moving to the cloud.

Source and more information:

https://www.securityweek.com/uk-government-releases-cloud-scada-security-guidance/

US sanctions APT31 hackers behind critical infrastructure attacks

The U.S. Treasury Department has sanctioned a Wuhan-based company used by the Chinese Ministry of State Security (MSS) as cover in attacks against U.S. critical infrastructure organizations.

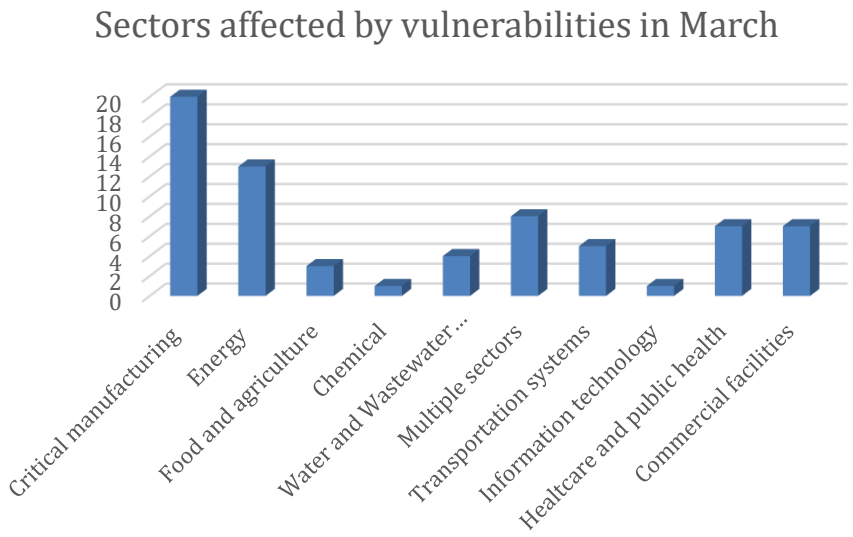
The Office of Foreign Assets Control (OFAC) has also designated two Chinese nationals (Zhao Guangzong and Ni Gaobin) linked to the APT31 Chinese state-backed hacking group and who worked as contractors for the Wuhan Xiaoruizhi Science and Technology Company, Limited (Wuhan XRZ) MSS front company for their involvement in the same attacks and "endangering U.S. national security." …

Source and more information:

https://www.bleepingcomputer.com/news/security/us-sanctions-apt31-hackers-behind-critical-infrastructure-attacks/

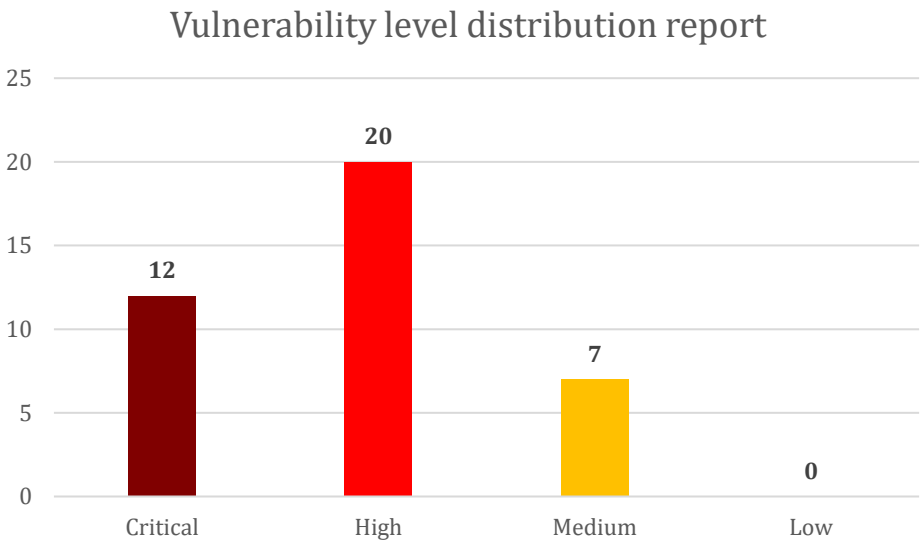
ICS vulnerabilities

In March 2024, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT and Siemens ProductCERT and Siemens CERT:



The most common vulnerabilities in March:

Vulnerability	CWE number	Items
Out-of-bounds Write	CWE-787	8
Out-of-bounds Read	CWE-125	6
Cross-site Scripting	CWE-79	5
Path Traversal	CWE-22	5
Uncontrolled Resource Consumption	CWE-400	4
Heap-based Buffer Overflow	CWE-122	4
Use After Free	CWE-416	4



ICSA-24-086-01: **Automation-Direct C-MORE EA9 HMI**

High level vulnerabilities: Path Traversal, Stack-Based Buffer Overflow, Plaintext Storage of a Password.

Automation-Direct C-MORE EA9 HMI | CISA

ICSA-24-086-02: **Rockwell Automation PowerFlex 527**

High level vulnerabilities: Improper Input Validation, Uncontrolled Resource Consumption.

Rockwell Automation PowerFlex 527 | CISA

ICSA-24-086-03: **Rockwell Automation Arena Simulation**

High level vulnerabilities: Out-of-bounds Write, Heap-based Buffer Overflow, Improper Restriction of Operations within the Bounds of a Memory Buffer, Use After Free, Access of Uninitialized Pointer, Out-of-bounds Read.

Rockwell Automation Arena Simulation | CISA

ICSA-24-086-04: **Rockwell Automation FactoryTalk View ME**

Medium level vulnerability: Cross-site Scripting.

Rockwell Automation FactoryTalk View ME | CISA

ICSA-24-081-01: **Advantech WebAccess/SCADA**

High level vulnerability: SQL Injection.

Advantech WebAccess/SCADA | CISA

ICSA-24-079-01: **Franklin Fueling System EVO 550/5000**

High level vulnerability: Path Traversal.

Franklin Fueling System EVO 550/5000 | CISA

SSA-968170: **Siemens SIMATIC STEP 7 V5.x and Derived Products (Update 1.2.)**

Critical level vulnerability: Improper Control of Generation of Code ('Code Injection').

SSA-968170 (siemens.com)

SSA-943925: **Siemens SINEC NMS before V2.0 SP1 (Update 1.1.)**

Critical level vulnerabilities: Multiple.

SSA-943925 (siemens.com)

SSA-871717: **Siemens Polarion ALM (Update 1.1.)**

High level vulnerabilities: Incorrect Default Permissions, Improper Authentication.

SSA-871717 (siemens.com)

SSA-711309: **Siemens SIMATIC Products (Update 1.6.)**

High level vulnerability: Integer Overflow or Wraparound.

SSA-711309 (siemens.com)

SSA-699386: **Siemens SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family before V4.5 (Update 1.2.)**

Critical level vulnerabilities: Out-of-bounds Read, Inadequate Encryption Strength, Double Free, NULL Pointer Dereference, Allocation of Resources Without Limits or Throttling, Acceptance of Extraneous Untrusted Data With Trusted Data, Use of Weak Hash, Direct Request ('Forced Browsing'), Unchecked Return Value, Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), Unsynchronized Access to Shared Data in a Multithreaded Context.

SSA-699386 (siemens.com)

SSA-693975: **Siemens Industrial Products (Update 1.1.)**

High level vulnerability: Missing Release of Memory after Effective Lifetime.

SSA-693975 (siemens.com)

SSA-592380: **Siemens SIMATIC S7-1500 CPUs and related products (Update 1.1.)**

High level vulnerability: Use After Free.

SSA-592380 (siemens.com)

SSA-552874: **Siemens SIPROTEC 5 Devices (Update 1.3.)**

Medium level vulnerability: Uncontrolled Resource Consumption.

SSA-552874 (siemens.com)

SSA-398330: **Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP V3.1 (Update 1.3.)** **Critical** level vulnerabilities: Multiple.

SSA-398330 (siemens.com)

SSA-322980: **Siemens SIPROTEC 5 Devices (Update 1.3.)**

High level vulnerability: NULL Pointer Dereference.

SSA-322980 (siemens.com)

SSA-000072: **Siemens Simcenter Femap (Update 1.1.)**

High level vulnerabilities: Out-of-bounds Write, Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Read, Access of Uninitialized Pointer.

SSA-000072 (siemens.com)

ICSA-24-074-01: **Siemens SENTRON 7KM PAC3x20**

Medium level vulnerability: Improper Access Control.

Siemens SENTRON 7KM PAC3x20 | CISA

ICSA-24-074-02: **Siemens Solid Edge**

High level vulnerability: Out-of-bounds Read.

Siemens Solid Edge | CISA

ICSA-24-074-03: **Siemens SINEMA Remote Connect Server**

Critical level vulnerabilities: Cross-site Scripting, Improper Access Control.

Siemens SINEMA Remote Connect Server | CISA

ICSA-24-074-04: **Siemens SINEMA Remote Connect Client**

Medium level vulnerability: Insertion of Sensitive Information into Externally-Accessible File or Directory.

Siemens SINEMA Remote Connect Client | CISA

ICSA-24-074-05: **Siemens RUGGEDCOM APE1808**

High level vulnerabilities: Heap-based Buffer Overflow, External Control of File Name or Path, Improper Privilege Management, Uncontrolled Resource Consumption, Improper Certificate Validation, Out-of-bounds Write, Use of Externally-Controlled Format String.

Siemens RUGGEDCOM APE1808 | CISA

ICSA-24-074-06: **Siemens SENTRON**

High level vulnerability: Hidden Functionality.

Siemens SENTRON | CISA

ICSA-24-074-07: **Siemens SIMATIC**

Critical level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Improper Input Validation, Missing Encryption of Sensitive Data, Incorrect Permission Assignment for Critical Resource, Expected Behavior Violation, Improper Authentication, Out-of-bounds Write, Use After Free, Inadequate Encryption Strength, Use of Insufficiently Random Values, Incorrect Authorization, Improper Locking, Improper Restriction of Rendered UI Layers or Frames, Improper Privilege Management, Missing Authorization, Cleartext Storage of Sensitive Information, Improper Check for Unusual or Exceptional Conditions, Improper Certificate Validation, Double Free, Integer Overflow or Wraparound, Out-of-bounds Read, Improper Initialization, Race Condition, Use of Uninitialized Resource, Improper Handling of Exceptional Conditions, Missing Initialization of Resource, Exposure of Resource to Wrong Sphere, Externally Controlled Reference to a Resource in Another Sphere, Injection, Excessive Iteration, Improper Preservation of Permissions, Improper Encoding or Escaping of Output, Incorrect Conversion between Numeric Types, Deserialization of Untrusted Data, Classic Buffer Overflow, Initialization of a Resource with an Insecure Default, Infinite Loop, Integer Underflow.

Siemens SIMATIC | CISA

ICSA-24-074-08: **Siemens SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Family**

Medium level vulnerabilities: Use of Hard-coded Cryptographic Key, Uncontrolled Resource Consumption.

Siemens SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Family | CISA

ICSA-24-074-09: **Siemens Sinteso EN Cerberus PRO EN Fire Protection Systems**

Critical level vulnerabilities: Classic Buffer Overflow, Out-of-bounds Read, Improper Restriction of Operations within the Bounds of a Memory Buffer.

Siemens Sinteso EN Cerberus PRO EN Fire Protection Systems | CISA

ICSA-24-074-10: **Siemens Siveillance Control**

Medium level vulnerability: Incorrect Authorization.

Siemens Siveillance Control | CISA

ICSA-24-074-11: **Siemens RUGGEDCOM APE1808 with Fortigate NGFW Devices**

Critical level vulnerabilities: Improper Certificate Validation, Cleartext Transmission of Sensitive Information, Path Traversal, Exposure of Sensitive Information to an Unauthorized Actor, Cross-site Scripting, Permissive List of Allowed Inputs, Relative Path Traversal, Improper Restriction of Excessive Authentication Attempts, Use of Externally-Controlled Format String, Access of Uninitialized Pointer, Out-of-bounds Write, Open Redirect, Improper Input Validation, Insertion of Sensitive Information into Log File, Heap-based Buffer Overflow, Insufficient Session Expiration, Improper Validation of Integrity Check Value, Improper Access Control, Infinite Loop, NULL Pointer Dereference, Stack-based Buffer Overflow, Basic XSS, Use of GET Request Method With Sensitive Query Strings, Interpretation Conflict, Use After Free, Improper Authorization.

Siemens RUGGEDCOM APE1808 with Fortigate NGFW Devices | CISA

ICSA-24-074-12: **Delta Electronics DIAEnergie**

High level vulnerabilities: Improper Authorization, SQL Injection, Path Traversal, Cross-site Scripting.

Delta Electronics DIAEnergie | CISA

ICSA-24-074-13: **Softing edgeConnector**

High level vulnerabilities: Cleartext Transmission of Sensitive Information, Path Traversal.

Softing edgeConnector | CISA

ICSA-24-074-14: **Mitsubishi Electric MELSEC-Q/L Series**

Critical level vulnerabilities: Incorrect Pointer Scaling, Integer Overflow or Wraparound.

Mitsubishi Electric MELSEC-Q/L Series | CISA

ICSA-23-143-03: **Mitsubishi Electric MELSEC Series CPU module (Update C)**

Critical level vulnerability: Classic Buffer Overflow.

Mitsubishi Electric MELSEC Series CPU module (Update C) | CISA

ICSA-24-072-01: **Schneider Electric EcoStruxure Power Design**

High level vulnerability: Deserialization of Untrusted Data.

Schneider Electric EcoStruxure Power Design | CISA

ICSA-24-067-01: **Chirp Systems Chirp Access**

Critical level vulnerability: Use of Hard-coded Credentials.

Chirp Systems Chirp Access | CISA

ICSA-24-065-01: **Nice Linear eMerge E3-Series**

Critical level vulnerabilities: Path traversal, Cross-site scripting, OS command injection, Unrestricted Upload of File with Dangerous Type, Incorrect Authorization, Exposure of Sensitive Information to an Authorized Actor, Insufficiently Protected Credentials, Use of Hard-coded Credentials, Cross-site Request Forgery, Out-of-bounds Write.

Nice Linear eMerge E3-Series | CISA

ICSMA-24-065-01: **Santesoft Sante FFT Imaging**

High level vulnerability: Out-of-Bounds Write.

Santesoft Sante FFT Imaging | CISA

ICSA-24-016-02: **Integration Objects OPC UA Server Toolkit (Update A)**

Medium level vulnerability: Improper Output Neutralization for Logs.

Integration Objects OPC UA Server Toolkit (Update A) | CISA

ICSA-24-060-01: **Delta Electronics CNCSoft-B**

High level vulnerability: Stack-based Buffer Overflow.

Delta Electronics CNCSoft-B | CISA

ICSMA-24-060-01: **MicroDicom DICOM Viewer**

High level vulnerabilities: Heap-based Buffer Overflow, Out-of-Bounds Write.

MicroDicom DICOM Viewer | CISA

The vulnerability reports contain more detailed information, which can be found on the following websites:

Cybersecurity Alerts & Advisories | CISA

CERT Services | Services | Siemens Siemens global website

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

CISA has published alerts in 2024 March:

CISA Adds Known Exploited Vulnerabilities to Catalog
CVE-2023-29360 Microsoft Streaming Service Untrusted Pointer Dereference Vulnerability;
CVE-2024-21338 Microsoft Windows Kernel Exposed IOCTL with Insufficient Access Control Vulnerability;
CVE-2023-21237 Android Pixel Information Disclosure Vulnerability;
CVE-2021-36380 Sunhillo SureLine OS Command Injection Vulnerablity;
CVE-2024-23225 Apple iOS and iPadOS Memory Corruption Vulnerability;
CVE-2024-23296 Apple iOS and iPadOS Memory Corruption Vulnerability;
CVE-2024-27198 JetBrains TeamCity Authentication Bypass Vulnerability;
CVE-2023-48788 Fortinet FortiClient EMS SQL Injection Vulnerability;
CVE-2021-44529 Ivanti Endpoint Manager Cloud Service Appliance (EPM CSA) Code Injection Vulnerability;
CVE-2019-7256 Nice Linear eMerge E3-Series OS Command Injection Vulnerability;
CVE-2023-24955 Microsoft SharePoint Server Code Injection Vulnerability;
Links and more information:
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds Two Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited JetBrains Vulnerability, CVE-2024-27198, to Catalog | CISA
CISA Adds Three Known Exploited Vulnerabilities to Catalog | CISA
CISA Adds One Known Exploited Vulnerability to Catalog | CISA

CISA and Partners Release Advisory on Threat Actors Exploiting Ivanti Connect Secure and Policy Secure Gateways Vulnerabilities
CISA and the following partners released joint Cybersecurity Advisory Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways:

- *Federal Bureau of Investigation (FBI)*
- *Multi-State Information Sharing & Analysis Center (MS-ISAC)*
- *Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)*
- *United Kingdom National Cyber Security Centre (NCSC-UK)*
- *Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment*
- *New Zealand National Cyber Security Centre (NCSC-NZ)*
- *CERT-New Zealand (CERT NZ)*

Links and more information:

CISA and Partners Release Advisory on Threat Actors Exploiting Ivanti Connect Secure and Policy Secure Gateways Vulnerabilities | CISA

CISA, FBI, and MS-ISAC Release Advisory on Phobos Ransomware

CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA), #StopRansomware: Phobos Ransomware, to disseminate known tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs), which are from incident response investigations tied to Phobos ransomware activity from as recently as February, 2024.

Links and more information:

CISA, FBI, and MS-ISAC Release Advisory on Phobos Ransomware | CISA

Cisco Releases Security Advisories for Cisco NX-OS Software

Cisco released security advisories to address vulnerabilities affecting Cisco NX-OS Software. A cyber threat actor could exploit one of these vulnerabilities to cause a denial-of-service condition.

Links and more information:

Cisco Releases Security Advisories for Cisco NX-OS Software | CISA

VMware Releases Security Advisory for Multiple Products

VMware released a security advisory to address multiple vulnerabilities in ESXi, Workstation, Fusion, and Cloud Foundation. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected system.

Links and more information:

VMware Releases Security Advisory for Multiple Products | CISA

Apple Releases Security Updates for iOS and iPadOS

Apple released security updates to address vulnerabilities in iOS and iPadOS. A cyber threat actor could exploit one of these vulnerabilities to obtain sensitive information.

Links and more information:

Apple Releases Security Updates for iOS and iPadOS | CISA

Cisco Releases Security Updates for Secure Client

Cisco released security updates to address vulnerabilities in Cisco Secure Client and Secure Client for Linux. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected device.

Links and more information:

Cisco Releases Security Updates for Secure Client | CISA

CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices

CISA and the National Security Agency (NSA) released five joint Cybersecurity Information Sheets (CSIs) to provide organizations with recommended best practices and/or mitigations to improve the security of their cloud environment(s).

Links and more information:

CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices | CISA

Apple Released Security Updates for Multiple Products

Apple released security updates to address vulnerabilities in Safari, macOS, watchOS, tvOS, and visionOS. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Apple Released Security Updates for Multiple Products | CISA

CISA Publishes SCuBA Hybrid Identity Solutions Guidance

CISA has published Secure Cloud Business Applications (SCuBA) Hybrid Identity Solutions Guidance (HISG) to help users better understand identity management capabilities and securely integrate their traditional on-premises enterprise networks with cloud-based solutions.

Links and more information:

CISA Publishes SCuBA Hybrid Identity Solutions Guidance | CISA

Fortinet Releases Security Updates for Multiple Products

Fortinet released security updates to address vulnerabilities in multiple Fortinet products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Fortinet Releases Security Updates for Multiple Products | CISA

Microsoft Releases Security Updates for Multiple Products

Microsoft has released security updates to address vulnerabilities in multiple products. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Microsoft Releases Security Updates for Multiple Products | CISA

Adobe Releases Security Updates for Multiple Products

Adobe released security updates to address multiple vulnerabilities in Adobe software. A cyber threat actor could exploit some of these vulnerabilities to take control of an affected system.

Links and more information:

Adobe Releases Security Updates for Multiple Products | CISA

Cisco Releases Security Updates for IOS XR Software

Cisco released security updates to address vulnerabilities in Cisco IOS XR software. A cyber threat actor could exploit one of these vulnerabilities to take control of an affected device.

Links and more information:

Cisco Releases Security Updates for IOS XR Software | CISA

Repository for Software Attestation and Artifacts Now Live

Software producers who partner with the federal government can now upload their Secure Software Development Attestation Forms to CISA's Repository for Software Attestation and Artifacts.

Links and more information:

Repository for Software Attestation and Artifacts Now Live | CISA

CISA and Partners Release Joint Fact Sheet for Leaders on PRC-sponsored Volt Typhoon Cyber Activity

CISA, the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and other U.S. and international partners are issuing a joint fact sheet, People's Republic of China State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders.

Partners of this publication include:

- *U.S. Department of Energy (DOE)*
- *U.S. Environmental Protection Agency (EPA)*
- *U.S. Transportation Security Administration (TSA)*
- *U.S. Department of Treasury*
- *Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC)*
- *Canadian Centre for Cyber Security (CCCS) a part of the Communications Security Establishment (CSE)*
- *United Kingdom's National Cyber Security Centre (NCSC-UK)*
- *New Zealand's National Cyber Security Centre (NCSC-NZ)*

Links and more information:

CISA and Partners Release Joint Fact Sheet for Leaders on PRC-sponsored Volt Typhoon Cyber Activity | CISA

Ivanti Releases Security Updates for Neurons for ITSM and Standalone Sentry
Ivanti has released security advisories to address vulnerabilities in Ivanti Neurons for ITSM and Standalone Sentry. A cyber threat actor could exploit these vulnerabilities to take control of an affected system.
Links and more information:
Ivanti Releases Security Updates for Neurons for ITSM and Standalone Sentry | CISA

CISA, FBI, and MS-ISAC Release Update to Joint Guidance on Distributed Denial-of-Service Techniques
CISA, the Federal Bureau of Investigation (FBI), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released an updated joint guide, Understanding and Responding to Distributed Denial-Of-Service Attacks, to address the specific needs and challenges faced by organizations in defending against DDoS attacks.
Links and more information:
CISA, FBI, and MS-ISAC Release Update to Joint Guidance on Distributed Denial-of-Service Techniques | CISA

CISA and FBI Release Secure by Design Alert to Urge Manufacturers to Eliminate SQL Injection Vulnerabilities
CISA and the Federal Bureau of Investigation (FBI) released a joint Secure by Design Alert, Eliminating SQL Injection Vulnerabilities in Software. This Alert was crafted in response to a recent, well-publicized exploitation of SQL injection (SQLi) defects in a managed file transfer application that impacted thousands of organizations. Additionally, the Alert highlights the prevalence of this class of vulnerability.
Links and more information:
CISA and FBI Release Secure by Design Alert to Urge Manufacturers to Eliminate SQL Injection Vulnerabilities | CISA

Apple Released Security Updates for Safari and macOS
Apple released security updates to address a vulnerability (CVE-2024-1580) in Safari and macOS. A cyber threat actor could exploit this vulnerability to take control of an affected system.
Links and more information:
Apple Released Security Updates for Safari and macOS | CISA

Cisco Releases Security Updates for Multiple Products
Cisco released security updates to address vulnerabilities in Cisco IOS, IOS XE, and AP software. A cyber threat actor could exploit some of these vulnerabilities to cause a denial-of-service.
Links and more information:
Cisco Releases Security Updates for Multiple Products | CISA

Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094

CISA and the open source community are responding to reports of malicious code being embedded in XZ Utils versions 5.6.0 and 5.6.1. This activity was assigned CVE-2024-3094. XZ Utils is data compression software and may be present in Linux distributions. The malicious code may allow unauthorized access to affected systems.

Links and more information:

Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094 | CISA